



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/805,018	03/19/2004	Scott R. Fisher	MFM-507	7775

7590 08/31/2007  
Frederick H. Gribbell  
FREDERICK H. GRIBBELL, LLC  
Suite 120  
10250 Alliance Road  
Cincinnati, OH 45242

EXAMINER
----------

SYED, NABIL H

ART UNIT	PAPER NUMBER
----------	--------------

2612

MAIL DATE	DELIVERY MODE
-----------	---------------

08/31/2007

PAPER

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

TH

<b>Office Action Summary</b>	<b>Application No.</b> 10/805,018	<b>Applicant(s)</b> FISHER, SCOTT R.	
	<b>Examiner</b> Nabil H. Syed	<b>Art Unit</b> 2612	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 19 March 2004.
- 2a) ☐ This action is **FINAL**.                      2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1-24 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-4, 6-11 and 13-24 is/are rejected.
- 7) ☐ Claim(s) 5 and 12 is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 19 March 2004 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All    b) ☐ Some \*    c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- |   |   |
|---|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)   | 4) <input type="checkbox"/> Interview Summary (PTO-413)<br>Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)                                  | 5) <input type="checkbox"/> Notice of Informal Patent Application                       |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)<br>Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____  |

## DETAILED ACTION

### *Claim Rejections - 35 USC § 103*

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

2. Claims 1-4, 6-11 and 13-16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Greenman (US Pub 2003/0179075) in view of Barrett et al. (5,046,084).

As of claim 1 and 6, Greenman discloses a method of operating an electronic lock box system (via property access system), said method comprising:

- (a) providing at least one electronic lock box having a secure compartment therein (via lock 101 having a key compartment 105; see fig. 1), a first computer circuit (via lock 101 having a microcontroller 119; see fig. 2), a first memory circuit (via microcontroller 119 having a memory section; see claim 2), a first device reader port, and a first data entry apparatus (via keyboard 102; see fig. 1);
- (b) providing a processing apparatus having a second computer circuit, a second memory circuit, a second device reader port, and a second data entry apparatus (via

Art Unit: 2612

property access system comprising a computer 420, which has a user interface to generate access code; see paragraph [33];

(d) at said second computer circuit (via performing the steps at the computer 420):

(i) determining a first present epoch time, determining a predetermined epoch time window for which a portable memory device will be valid (note: Greenman discloses that the user will enter the date and time of the appointment and how long the appointment will last, for example ½ hour or 1 hour in the computer system 420; so determining the time window for which the access code will be valid; see paragraph [0052]; determining a first cryptographic seed value for use with a data encryption function, and determining a user's first identification code (via using the encrypted version of the agent code (user identification number) with the encrypted version of the lock serial number which is known to the computer and the lock, to generate a diversified access code; see paragraph [0052]);

(ii) using data encryption function, calculating a diversified value based upon both said first cryptographic seed value and said user's first identification code (see paragraph [0052]);

(iii) coupling said portable memory device to said second device reader port, and communicating said diversified value to said portable memory device;

(e) at said at least one electronic lock box (via performing the function in the lock 101):

(ii) determining a second present epoch time, determining a second cryptographic seed value; and determining a user's second identification code from a manual entry at said first data entry apparatus (via agent entering his/her agent code and encrypted entry

Art Unit: 2612

code; the lock determines different time intervals to check if it is the valid time to allow the access; see paragraph [0053]);

(iii) using data encryption function, decrypting first diversified value based upon second cryptographic seed value, resulting in a third identification code (via the lock decrypting the encrypted agent code and encrypted version of the entry code, and coming up with 14 different access codes; and

(iv) comparing said user's second identification code and said third identification code, and if they match, permitting access to secure compartment (via the lock comparing the 14 access codes with the one entered by the user and if any one of those 14 access codes matches with the one entered by the user permitting access to the property; see paragraph [0054]-[0060]).

However Greenman fails to disclose a portable memory device having a memory circuit and at least one electrical conductor for communicating with a device port.

Barrett discloses an electronic real estate lockbox system 10 that has an electronic key 14, a lockbox with a key safe 12, and a computer 18 (see fig. 1). The system 10 also has stand 16, which is used to interface computer 18 with the lockbox and key unit. The user uses the computer to save the codes inside the key and then the key is used to access the lock (see col. 3, lines 13-25). Barrett discloses that the key 14 is a data key, comprising a CPU 52, keypad 48, memory 56, and a battery 60 (see fig. 14; also see col. 5, lines 44-49).

From the teaching of Barrett it would have been obvious to one having ordinary skill in the art at the time the invention to modify the property access system of

Art Unit: 2612

Greenman to include an electronic key to open the lockbox as taught by Barrett in order to improve the real state business so when a key and lockbox are engaged, data about the current transaction and previous transaction can be stored in the key and later it can be transferred to the main computer inside the main office, so the main office can have all the record of the transaction like which agent visited the premise, when did he/she visit, what time did they visit etc (see col. 41, lines 52-57).

As of claim 2, Greenman discloses that the user's identification code to access the lock is valid within a predetermined time and user must get a new code to access the lock at a different time period (see paragraph [0008]).

As of claim 3, Greenman discloses that the determining a first cryptographic seed value comprises: dividing said present epoch time by said predetermined epoch time window (see paragraph [0050]-[0052]).

As of claim 4, Greenman discloses that different encryption techniques can be used to encrypt the code to make a unique encryption key (Note: Greenman discloses that lock 101 apply DES or AES encryption algorithm, and in encryption it is well known to encrypt the codes with the random numbers so it is hard for any one to break into the system; see paragraphs [0014], [0035], [0066]).

As of claim 7, Greenman discloses a method of operating an electronic lock box system, said method comprising:

- (a) providing a central database computer (via computer system 420; see fig. 5) and an electronic lock box at a second physical location (via lock 101; see fig. 5);
- (b) encrypting, at a first real time, a user's identification number using a first encryption

Art Unit: 2612

seed value that is known only to central database computer and to electronic lock box, wherein said first encryption seed value is time dependent (via computer system 420, creating an encrypted access code using the date/time, user identification number and the lock serial number which is known to the lock and the user. Greenman also discloses that the lock 101 and computer system 420 both have same algorithm operating on both electronic devices; see paragraph [0029], lines 1-4; also see paragraph [0052]);

(c) storing encrypted user's identification number on a portable memory apparatus at said central database computer;

(d) transferring said encrypted user's identification number from said portable memory apparatus to said electronic lock box;

(e) decrypting, at a second real time, said encrypted user's identification number using a second encryption seed value, thereby resulting in a decrypted ID value (via the lock decrypting at a second time, the encrypted version of agent and locks serial number and resulting in a decrypted ID value; see paragraph [0053]);

(d) comparing said decrypted ID value to data entered on a keypad at said electronic lock box, and if the data matches said decrypted ID value, allowing access to a secure compartment within said electronic lock box (via the microcontroller comparing the decrypted ID values with the entered identification number and allowing the access to the compartment if the ID's match; see paragraph [0060]).

However Greenman fails to disclose that a portable memory device having a memory circuit and at least one electrical conductor for communicating with a device port.

Barrett discloses an electronic real estate lockbox system 10 that has an electronic key 14, a lockbox with a key safe 12, and a computer 18 (see fig. 1). The system 10 also has stand 16, which is used to interface computer 18 with the lockbox and key unit. The user uses the computer to save the codes inside the key and then the key is used to access the lock (see col. 3, lines 13-25).

From the teaching of Barrett it would have been obvious to one having ordinary skill in the art at the time the invention to modify the property access system of Greenman to include an electronic key to open the lockbox as taught by Barrett in order to improve the real state business so when a key and lockbox are engaged, data about the current transaction and previous transaction can be stored in the key and later it can be transferred to the main computer inside the main office, so the main office can have all the record of the transaction like which agent visited the premise, when did he/she visit, what time did they visit etc (see col. 41, lines 52-57).

As of claim 8, Greenman discloses that the data entered on the keypad at electronic lock box is equal to user's identification number (via real estate agent entering his/her agent code which is a unique identification code assigned to that specific agent; see paragraph [0053]).

As of claim 9, Greenman discloses that the decrypted code will match the access code if the user enters the code within a predefined time, for example if a real estate



agent has appointment at 10:00 AM he/she will have to enter the codes to access the lock within a predetermined time interval set around 10:00 AM (see paragraph [0053]-[0058]).

As of claim 10, Greenman discloses that the determining a first cryptographic seed value comprises: dividing said present epoch time by said predetermined epoch time window (see paragraph [0050]-[0052]).

As of claim 11, Greenman discloses that different encryption techniques can be used to encrypt the code to make a unique encryption key (Note: Greenman discloses that lock 101 apply DES or AES encryption algorithm, and in encryption it is well known to encrypt the codes with the random numbers so it is hard for any one to break into the system; see paragraphs [0014], [0035], [0066]).

As of claim 13 and 16, Greenman discloses an electronic lock box apparatus, comprising: an electrical power source (via the lock 101 receiving the power from a battery; see paragraph [0063]), a controller circuit (via controller 119; see fig. 1), a secure compartment having an access member actuated by a prime mover apparatus (via key compartment 105; see fig. 1), a manual data entry apparatus (via keyboard 102), and a device reader port; and

wherein, said controller circuit is configured:

(a) to determine a present epoch time, to determine a predetermined epoch time window for which said portable memory device will be valid, to determine a cryptographic seed value for use with a data encryption algorithm (via the controller 119 of the lock determining the time window for which the access to the lock is granted.

Note: Greenman discloses that lock 101 apply DES or AES encryption algorithm, and in encryption it is well known to encrypt the codes with the random numbers so it is hard for any one to break into the system; see paragraph [0066];

(c) to decrypt first data value using data encryption algorithm, based upon cryptographic seed value, thereby determining a second data value (Greenman discloses that the user enters the encrypted serial number of the lock into the lock and lock decrypt the number using the same algorithm as was used by the computer system 420 to encrypt the code; see paragraph [00053]; ;

(d) to receive a user's identification code that is entered at said manual entry apparatus (via agent entering his/her agent code through keyboard 102; see paragraph [0053]);

(e) to compare said user's identification code to said second data value (via comparing the entered code with the decrypt ID codes; see paragraph [0060]; and

(f) if said user's identification code is equal to said second data value, to allow access to said secure compartment by actuating prime mover apparatus to open access member (via opening up the key compartment 105, if the code entered by the user matches the decrypted code; see paragraph [0060]).

However Greenman fails to disclose that a portable memory device having a memory circuit and at least one electrical conductor for communicating with a device port.

Barrett discloses an electronic real estate lockbox system 10 that has an electronic key 14, a lockbox with a key safe 12, and a computer 18 (see fig. 1). The system 10 also has stand 16, which is used to interface computer 18 with the lockbox

and key unit. The user uses the computer to save the codes inside the key and then the key is used to access the lock (see col. 3, lines 13-25). Barrett also discloses that the key 14 is a data key, comprising a CPU 52, keypad 48, memory 56, and a battery 60 (see fig. 14; also see col. 5, lines 44-49).

From the teaching of Barrett it would have been obvious to one having ordinary skill in the art at the time the invention to modify the property access system of Greenman to include an electronic key to open the lockbox as taught by Barrett in order to improve the real state business so when a key and lockbox are engaged, data about the current transaction and previous transaction can be stored in the key and later it can be transferred to the main computer inside the main office, so the main office can have all the record of the transaction like which agent visited the premise, when did he/she visit, what time did they visit etc (see col. 41, lines 52-57).

As of claim 14, Greenman discloses a central computer apparatus (via computer system 420; see fig. 5); and wherein first data value is calculated by central computer apparatus, which is configured to:

i) determining a second present epoch time, determining a predetermined epoch time window for which a portable memory device will be valid (note: Greenman discloses that the user will enter the date and time of the appointment and how long the appointment will last, for example ½ hour or 1 hour in the computer system 420; so determining the time window for which the access code will be valid; see paragraph [0052];, determining a second cryptographic seed value for use with a data encryption function, and determining a user's first identification code (via using the encrypted version of the

agent code (user identification number) with the encrypted version of the lock serial number which is known to the computer and the lock, to generate a diversified access code; see paragraph [0052] ;

(ii) using said data encryption function, calculating a diversified value based upon both said first cryptographic seed value and said user's first identification code (see paragraph [0052]);

However Greenman fails to disclose that a portable memory device having a memory circuit and at least one electrical conductor for communicating with a device port.

Barrett discloses an electronic real estate lockbox system 10 that has an electronic key 14, a lockbox with a key safe 12, and a computer 18 (see fig. 1). The system 10 also has stand 16, which is used to interface computer 18 with the lockbox and key unit. The user uses the computer to save the codes inside the key and then the key is used to access the lock (see col. 3, lines 13-25).

From the teaching of Barrett it would have been obvious to one having ordinary skill in the art at the time the invention to modify the property access system of Greenman to include an electronic key to open the lockbox as taught by Barrett in order to improve the real state business so when a key and lockbox are engaged, data about the current transaction and previous transaction can be stored in the key and later it can be transferred to the main computer inside the main office, so the main office can have all the record of the transaction like which agent visited the premise, when did he/she visit, what time did they visit etc (see col. 41, lines 52-57).

As of claim 15, Greenman discloses that the user's identification code to access the lock is valid within a predetermined time and user must get a new code to access the lock at a different time period (see paragraph [0008]).

3. Claims 17-24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lavelle et al. (5,923,264) in view of Greenman (US Pub 2003/0179075).

As of claim 17, Lavelle discloses an electronic lock box apparatus (electronic lock assembly 10; see fig. 1), comprising: an electrical power source (via power source 78; see col. 4, lines, 52-56) a controller circuit (via lock controller 76; see col. 4, lines 57-67; see fig. 1 and fig. 4), a secure compartment having an access member actuated by a prime mover apparatus (via key compartment 105; see fig. 1), a manual data entry apparatus (via case 34 comprising keypad 42; see fig. 3A) and a device reader port (via case 34 comprising a electronic reader 44; see fig. 3A);

(a) to determine whether said electronic lock box apparatus is presently in one of (i) a first, higher security state and (ii) a second, lower security state (note: higher security state is defined when the user has to use both keypad and card code to access the lock and lower security state is when user uses only key pad to enter the access code.

Lavelle discloses that lock controller checks to see if the initial contact was a key closure on the key pad 42 (see col. 5, lines 54-55) and if the key closure was a data chip input at electronic reader 44;

(b) if said electronic lock box apparatus is presently in said second, lower security state, access may be obtained by a proper code, provided through manual data entry apparatus (via microprocessor of lock controller comparing the input from the key pad

with valid personal access codes which are stored in the memory and allowing the access to the lock; see col. 6, lines 50-54); and

(c) if electronic lock box apparatus is presently in first, higher security state, access may be obtained by a combination of a proper user's identification code, provided through manual data entry apparatus, and by decrypting a diversified data value from a portable memory device, received through device reader port (via electronic lock assembly configured to unlock only on entry of both a personal access code on keypad 42 and an electronic access code with the electronic reader 44; see col. 7, lines 12-21).

However Lavelle fails to explicitly disclose a secure compartment having an access member actuated by a prime mover apparatus.

Greenman discloses a property access system comprising a portable lock 101 having a secure compartment (via a key compartment 105; see fig. 1a; also see paragraph [0026], lines 9-12).

From the teaching of Greenman it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify the lock assembly of Lavelle to include a secure compartment as taught by Greenman in order to improve the functionality of the electronic locking mechanism to which are employed with secured doors to and/or from buildings, secured access points and/or containers including secure storage devices for the delivery and pickup of goods. The secure compartment can also be used to contain house keys, business cards written messages and the like (see col. 3, lines 30-32).

As of claim 18, Lavelle discloses that the memory 84 of the lock 10 can be programmed to store valid personal access code and valid "key" code (see col. 4, lines 66-67 and col. 5, lines 1) and a real time clock and audit trail memory 104 communicate with the microprocessor to record the chronological history of each attempted lock/unlock event and the associated access code entered (see col. 5, lines 22-26).

As of claim 19, Lavelle discloses that the access code is static code that does not change over the passage of time (note: Lavelle discloses that the personal access codes can be assigned to the students in a university to access their dormitory room, since students will use the same code to enter the room, so the code is a static code that does not change over the passage of time; see col. 2, lines 26-30).

However Lavelle fails to disclose a progressive code that changes over the passage of time.

Greenman discloses that the access code to open the lock 101 is valid for only for a specified time interval for a specified user and each user must get a new authorized code to enter at a different time period; (see paragraph [0008]).

From the teaching of Greenman it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify the lock assembly of Lavelle to include the feature of having a progressive code as taught by Greenman in order to allow only specific people access to the property only a authorized times. People the people who have accessed the property in the past do not have access of the property at a later time unless given authorization for the new time period, so the maintenance people have only access to the rooms of the student for a specified time

and they do not have access to the premise any other time, keeping the students privacy secure; see paragraph [0002], lines 4-7).

As of claim 20, Lavelle discloses that a student is provided with an access code to access the dormitory room (so the school administrator, or who ever handles the school security assigns the codes to the students and puts the lock in the function to receive the code through the keypad to lock/unlock the lock 101; see col. 2, lines 24-32).

As of claim 21, Lavelle discloses that the user uses a "key" to enter the code into the electronic reader, and they key may be a magnetic card, microchip contact device or other electromagnetic device 9see col. 1, lines 54-55).

As of claim 22, Lavelle discloses that the electronic lock assembly 10 can be configured to unlock only on entry of both a personal access code and an electronic assess code with the electronic reader. So when the security administrators of a university assign an access code to a student or a maintenance person, they can enable the function of the lock so the lock will open only when user provides a proper access code through the keypad 42 and a valid electronic key through the electronic reader 44; see col. 7, lines 12-21). Lavelle also discloses that a privacy button 106 mounted to the rear assemble can be included to prevent actuation of the lock from the exterior side regardless of the input entered at the reader 42 and 44; see col. 5, lines 26-29).

As of claim 23, Lavelle discloses that if said electronic lock box apparatus is set up so as to permit an other user to obtain access to while in its second, lower security state, then authorized user may choose to set up the electronic lock box apparatus,



upon such access of the secure compartment, to one of:

(a) automatically change a mode of said electronic lock box apparatus from second, lower security state to the first, higher security state (Note: higher security state is defined when the user has to use both keypad and card code to access the lock.

Lavelle discloses that electronic lock assembly configured to unlock only on entry of both a personal access code on keypad 42 and an electronic access code with the electronic reader 44; see col. 7, lines 12-21. So when the security administrators of a university assign an access code to a student or a maintenance person, they can enable the function of the lock so the lock will open only when user provides a proper access code through the keypad 42 and a valid electronic key through the electronic reader 44; see col. 7, lines 12-21); and

(b) keep the mode of electronic lock box apparatus in second, lower security state (Note: lower security state is when user uses only key pad to enter the access code. Lavelle discloses that microprocessor of lock controller comparing the input from the key pad with valid personal access codes which are stored in the memory and allowing the access to the lock; see col. 6, lines 50-54);.

As of claim 24, Lavelle discloses the electronic lock box further comprising a shackle member that is attachable to and detachable from said electronic lock box (via lock assembly comprising a latch 18), shackle member being actuated by prime mover apparatus as directed by said controller circuit (via electronically lock 10 comprising an electrically controlled motorized drive unit 15 including a motor 28 for operating the cylindrical lock 14 to lock the latch 18 (see col. 3, lines 50-48-52) and microprocessor

Art Unit: 2612

86 of the lock controller control the motor 28 to lock or unlock the electronic lock (see col. 5, lines 7-10);

wherein: if authorized user operates prime mover apparatus to detach shackle from electronic lock box at a time when the electronic lock box is in said second, lower security state, then controller will automatically change a mode of electronic lock box to first, higher security state (Note: Lavelle discloses that the electronic lock can be configured to unlock using both readers 42 and 44 on the lock for all the users or only for certain door lock users such as security personnel. So when the lock is configured to unlock with the keypad for students of a university and using an access code and a memory card for security personnel, when the students unlock the lock using their codes and lock the electronic lock when they leave the room, the lock automatically moves into the higher security upon the students locking the door because now if a security personnel want to unlock the lock he/she have to use both keys to enter the room.

***Allowable Subject Matter***

4. Claims 6 and 12 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

### ***Conclusion***

5. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Kucharczyk (US Pub 2001/0050615) discloses a locking device, which uses cryptographically strong pseudo-random number generator as part of its access code entry unit (see paragraph [0044]).

Frolov et al. 96,714,118) discloses a modular electronic door security system that uses a keypad and an electronic key to open the door (see fig. 5A).

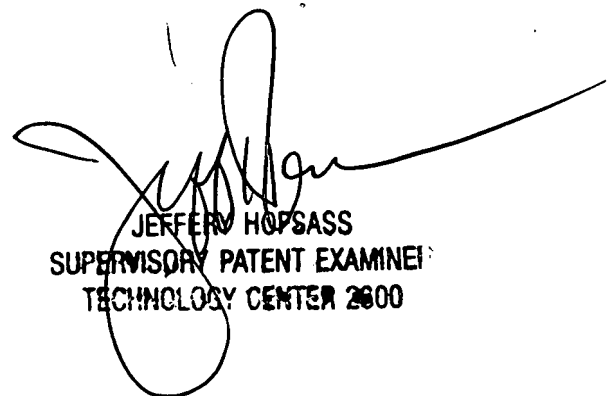
Any inquiry concerning this communication or earlier communications from the examiner should be directed to Nabil H. Syed whose telephone number is 571-270-3028. The examiner can normally be reached on M-F 7:30-5:00 alt Friday off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jeffery A. Hofsass can be reached on (571) 272-2981. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Nabil H Syed  
Examiner  
Art Unit 2612

N.S



JEFFERY HOPSASS  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2600